

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application for:

DEFAULT ENCRYPTION AND DECRYPTION

Inventor(s): Leo Mark Pedlow, Jr. and Davender Agnihotri

Docket Number: SNY-T5718.02

Prepared By:

Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606

Phone: (919) 816-9981
Fax: (919) 816-9982
Email: miller@patent-inventions.com

CERTIFICATE OF EXPRESS MAILING FOR NEW PATENT APPLICATION

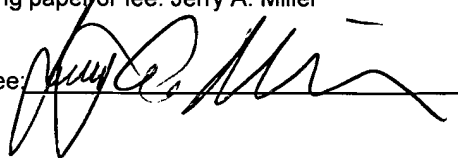
"Express Mail" mailing label number: ER 999163718 US

Date of Deposit: March 8, 2004

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name of person mailing paper or fee: Jerry A. Miller

Signature of person mailing paper or fee:

A handwritten signature in black ink, appearing to read "Jerry A. Miller", is written over a horizontal line.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEFAULT ENCRYPTION AND DECRYPTION

CROSS REFERENCE TO RELATED DOCUMENTS

This application claims priority benefit of U.S. Provisional Patent Application Serial No. 60/516,712, to Pedlow, Jr. et al., filed Nov. 3, 2003 entitled "Method for Continuous Delivery of Secure Digital Content", which is hereby incorporated by reference. This application is also related to patent applications docket number SNY-R4646.01 entitled "Critical Packet Partial Encryption" to Unger et al., serial number 10/038,217; patent applications docket number SNY-R4646.02 entitled "Time Division Partial Encryption" to Candelore et al., serial number 10/038,032; docket number SNY-R4646.03 entitled "Elementary Stream Partial Encryption" to Candelore, serial number 10/037,914; docket number SNY-R4646.04 entitled "Partial Encryption and PID Mapping" to Unger et al., serial number 10/037,499; and docket number SNY-R4646.05 entitled "Decoding and Decrypting of Partially Encrypted Information" to Unger et al., serial number 10/037,498 all of which were filed on January 2, 2002 and are hereby incorporated by reference herein.

COPYRIGHT NOTICE

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the

1 facsimile reproduction of the patent document or the patent disclosure, as it
2 appears in the Patent and Trademark Office patent file or records, but otherwise
3 reserves all copyright rights whatsoever.

4 5 **BACKGROUND**

6 **FIGURE 1** shows one possible configuration of a DVB system 100. This
7 example system complies with the Digital Video Broadcast (DVB) specification
8 (but the inventions disclosed hereinafter are not necessarily limited to such
9 systems). Accordingly, all components and interfaces are described in detail in
10 the DVB specification. The detail that is presented here is for background
11 informational use. The reader is referred to the DVB specification for specific
12 details beyond those needed for the intended overview presented here.

13 In **FIGURE 1**, cable system 100 is shown. Content Encryption Block 104,
14 conditional access system 108 and television Set-Top Box STB 112 are also
15 shown. Within content encryption block 104 (content encryption block 104 and
16 CA system 108 are generally located at the cable system headend or content
17 distribution broadcast center) are Simulcrypt™ Synchronizer (SCS) Processor
18 116 and content encryption block 120. Within the content encryption block 120
19 are code word generator 124 and encrypt engine 128. Output multiplexer (mux)
20 132 is the final block within content encryption block 104. Details of the
21 communications interfaces within cable system head end will follow. The
22 interfaces described may be hardware interfaces with direct connections as
23 shown or software interfaces for communication over, for example, a bus
24 structure without limitation.

25 Within conditional access system 108 are the content scheduler 136, the
26 event information scheduler (EIS) 140, the subscriber database 144, the ECM
27 generator 148 and the EMM generator 152.

28 With the major components identified so far, an example DVB encryption
29 cycle can be discussed. Clear content 156 is received by encrypt engine 128 on

1 content interface 160. Likewise, the current code word (or encryption key(s)) is
2 received by encrypt engine 128 from code word generator 124 on codeword
3 interface 164. The same codeword is transferred from code word generator 124
4 to SCS processor 116 on code word interface 168.

5 Communications between the content encryption block 104 and
6 conditional access system 108 occurs over the encryption device to conditional
7 access system communications link 172. Conditional access system
8 communications link 172 is composed of several other interfaces, namely access
9 criteria interface 176, code word and access criteria interface 180 and signed
10 ECM interface 184.

11 During the typical DVB encryption cycle, EIS 140 receives information
12 from content scheduler 136 on content schedule interface 188 and transmits this
13 information to SCS processor 116 on access criteria interface 176. SCS
14 processor 116 then transmits the code word received from code word generator
15 124 on code word interface 168 and the access criteria received from EIS 140 on
16 access criteria interface 176 to ECM generator 148 across code word and
17 access criteria interface 180.

18 Likewise, EMM generator 152 interfaces with subscriber database 144
19 across subscriber database interface 192 to retrieve information necessary to
20 create EMM messages. ECM generator 148 and EMM generator 152
21 communicate across ECM/EMM interface 196 to communicate information that is
22 necessary for ECM generator 148 to create signed ECM messages. EMM
23 packets are transferred to STB 112 across EMM packet interface 1100 and
24 signed ECM messages are transferred from ECM generator 148 to SCS
25 processor 116 across signed ECM interface 184 to complete the current actions
26 of the conditional access system 108.

27 SCS processor 116 then asserts a period switch command to the encrypt
28 engine 128 across period switch interface 1104. Encrypt engine 128 then
29 outputs an encrypted stream of data on interface 1108 to output MUX 132 while

1 SCS processor 116 transmits the signed ECM message (intended to be placed
2 into the outgoing transport stream) across signal ECM insertion interface 1112 to
3 output MUX 132. The final encrypted transport stream with ECMs inserted is
4 then output from content encryption block 104 on transport stream interface
5 1116. Keep in mind that transport stream interface can be any of a cable
6 network, satellite connectivity, or any other suitable communication medium.

7 At STB 112, the transport stream is received and ECM processor 1120
8 strips out the ECM packets from 1116. The raw transport packets are passed
9 along transport packet interface 1124 to the Cryptoperiod switch 1128, which
10 switches periodically between even decrypt engine 1132 and odd decrypt engine
11 1136. EMM packets are received on EMM packet interface 1100 (again any
12 suitable communication medium, for example an out of band delivery mechanism
13 per the DVB specification, connects EMM generator 152 and ECM processor
14 1120) by ECM processor 1120. A recovered code word is output to both the
15 even decrypt engine 1132 and the odd decrypt engine 1136 across recovered
16 code word interface 1140. Finally, clear transport data is transmitted to the
17 digital decoder 1144 across clear transport interface 1148.

18 Many details of timing and forwarding of codewords and other interactions
19 between the components of the system have been omitted to simplify the
20 previous discussion. The reader is again referred to the DVB specification for
21 specific details of the components, interfaces, and relevant timings. It is believed
22 sufficient for the purposes of this disclosure to generally understand the
23 architecture, as presented herein, with reference to the DVB specification for
24 specific details.

25 The Passage™ initiative, promoted by Sony, provides a mechanism for
26 MSOs to deploy non-legacy headend equipment, subscriber devices and
27 services on their existing legacy networks. In the USA, these networks are
28 supplied by either Motorola (former General Instrument) or Scientific Atlanta.
29 These two companies at present constitute better than a 99% share of the US

1 cable system market as turnkey system providers. The systems, by design,
2 employ proprietary technology and interfaces precluding the introduction of non-
3 incumbent equipment into the network. An MSO, once choosing one of these
4 suppliers during conversion from an analog cable system to a digital cable
5 system, faces a virtual monopoly when seeking suppliers for additional
6 equipment as their subscriber base or service offering grows.

7 Before the Passage™ initiative, the only exit from this situation was to
8 forfeit the considerable capital investment already made with the incumbent
9 provider, due to the intentional incompatibility of equipment between the
10 incumbent and other sources. One primary barrier to interoperability is in the
11 area of conditional access systems, the heart of addressable subscriber
12 management and revenue collection resources in a modern digital cable network.

13 The Passage™ technologies were developed to allow the independent
14 coexistence of two or more conditional access systems on a single, common
15 plant. Unlike other attempts to address the issue, the two systems operate with a
16 common transport stream without any direct or indirect interaction between the
17 conditional access systems. The basic processes used in these technologies are
18 discussed in detail in the above-referenced pending patent applications.

19 The above-referenced commonly owned patent applications, and others,
20 describe inventions relating to various aspects of methods generally referred to
21 herein as partial encryption or selective encryption, consistent with certain
22 aspects of Passage™. More particularly, systems are described therein wherein
23 selected portions of a particular selection of digital content are encrypted using
24 two (or more) encryption techniques while other portions of the content are left
25 unencrypted. By properly selecting the portions to be encrypted, the content can
26 effectively be encrypted for use under multiple decryption systems without the
27 necessity of encryption of the entire selection of content. In some embodiments,
28 only a few percent of data overhead is consumed to effectively encrypt the
29 content using multiple encryption systems. This results in a cable or satellite

1 system being able to utilize Set-top boxes (STB) or other implementations of
2 conditional access (CA) receivers from multiple manufacturers in a single system
3 - thus freeing the cable or satellite company to competitively shop for providers of
4 Set-top boxes.

5 In each of these disclosures, the clear content is identified using a primary
6 Packet Identifier (PID). A secondary PID (or shadow PID) is also assigned to the
7 program content. Selected portions of the content are encrypted under two (or
8 more) encryption systems and the encrypted content transmitted using both the
9 primary and secondary PIDs (one PID or set of PIDs for each encryption
10 system). The so-called legacy STBs operate in a normal manner decrypting
11 encrypted packets arriving under the primary PID and ignoring secondary PIDs.
12 The newer (non-legacy) STBs operate by associating both the primary and
13 secondary PIDs with a single program. Packets with a primary PID are decoded
14 normally and packets with a secondary PID are first decrypted then decoded.
15 The packets associated with both PIDs are then assembled together to make up
16 a single program stream. The PID values associated with the packets are
17 generally remapped to a single PID value for decoding (shadow PIDs remapped
18 to the primary PID value or vice versa.)

19 In certain encrypted digital broadcast transmission systems, regardless of
20 the delivery medium (cable, DBS, DSL, etc.), content at some point prior to
21 transmission to the terminal devices passes through an encryption device
22 designed to obscure the digital content from unauthorized access. These
23 devices use published encryption algorithms such as DES, DES-ECB, DVB-CSA,
24 AES and other methods such as proprietary encryption systems, and typically
25 are dynamically managed by a conditional access system that manages all the
26 encryption devices in a facility. The conditional access system determines which
27 services on each transport should be encrypted and supplies the access criteria,
28 which are the credentials that each particular subscriber terminal device must
29 possess in order to access and display the material. The actual key used by the

1 encryption device to encrypt the data stream passing through the device,
2 depending upon component and system vendor, may either be supplied by the
3 encryption device or the conditional access system itself.

4 The conditional access system also is responsible for forming special
5 messages sent to the subscriber terminal devices, called entitlement control
6 messages (ECMs) that contain the content encryption key and the access criteria
7 for the content. The data payload in the ECM is itself encrypted, but using a
8 different algorithm than the content itself. The ECM encryption algorithm is a
9 proprietary technology of the conditional access system provider and a closely
10 guarded secret. The ECMs can be inserted in the transport stream at the
11 encryption device or sent through other means and are used by the conditional
12 access agent inside each subscriber terminal device to recover the content
13 encryption key, if authorized for viewing, and supply it the transport decryption
14 element in the terminal device to recover the clear-text content.

15 In a DVB based system, the conditional access system supplies the
16 access criteria to an element, which may be integrated within the encryption
17 device itself, called a Simulcrypt synchronizer (SCS). The SCS manages the
18 timing and delivery of data between the key generator, ECM inserter and stream
19 encryption engine, which can be elements within the encryption device and the
20 conditional access management system, external to the encryption device.

21 The conditional access management system provisions the encryption
22 device, indicating the MPEG services within the processed transport stream(s) to
23 encrypt. This indication can either be at the service or at the component level
24 and according to the MPEG transport protocol, a service may contain any
25 combination of encrypted and clear elementary stream components. When the
26 encryption device determines that the system key period (cryptoperiod) is near
27 expiration, the key generator creates a new random key to be used to encrypt or
28 "sign" the service components that are being encrypted. This new key is
29 delivered to the SCS. In parallel, the conditional access management system

1 delivers the access criteria associated with a particular MPEG service to the SCS
2 as well. The access criteria changes relatively infrequently, as often as once per
3 one to two hours for pay-per-view content, to as seldom as monthly or yearly (or
4 longer) in the case of advertising-based subscription television services where
5 the only reason for encryption is to stop non-cable customers from stealing
6 service. An example of the latter might be the Discovery Channel or TLC
7 services, as opposed to true subscription (HBO or Showtime) or pay-per-view
8 services, which carry no supporting advertising and revenues are derived from
9 subscriptions for the content itself.

10 The SCS retains the access criteria supplied by the conditional access
11 management system for each encrypted service until either the service is
12 provisioned for non-encrypted delivery (clear service) or the data is superseded
13 with newer access criteria. Whenever the key generator delivers a new key to
14 the SCS, it bundles the key and current access criteria for the encrypted service
15 and sends this prototype message to the entitlement control message generator
16 (ECMG), part of the conditional management system, for encryption or "signing"
17 with the proprietary algorithm as described earlier. The signed ECM is sent by
18 the ECMG back to the SCS in the encryption device. The SCS takes the
19 delivered ECM and places the new ECM in the outgoing, encrypted transport
20 stream. After a predetermined period to allow time for subscriber terminal
21 devices to recover and decode the new ECM message, the SCS then issues the
22 new key to the stream encryption engine as a replacement for the old key in the
23 encryption of the indicated service. This entire process is repeated every
24 cryptoperiod (seconds) and is performed in parallel within the encryption device
25 for each indicated service in the transport multiplex processed by the device
26 since no two services use the same key. The conditional access management
27 system independently delivers access criteria for every encrypted service in the
28 channel plan as well as performing ECM signing for each encrypted service
29 every cryptoperiod.

1 **BRIEF DESCRIPTION OF THE DRAWINGS**

2 The features of the invention believed to be novel are set forth with
3 particularity in the appended claims. The invention itself however, both as to
4 organization and method of operation, together with objects and advantages
5 thereof, may be best understood by reference to the following detailed
6 description of the invention, which describes certain exemplary embodiments of
7 the invention, taken in conjunction with the accompanying drawings in which:

8 **FIGURE 1** is a block diagram of a typical pre-existing cable system.

9 **FIGURE 2** is a block diagram of a cable system head end consistent with
10 certain embodiments of the present invention.

11 **FIGURE 3** is a flow diagram of a cable system head end consistent with
12 certain embodiments of the present invention.

13 **FIGURE 4** is a block diagram of a cable system consistent with certain
14 embodiments of the present invention.

15 **FIGURE 5** is a flow diagram of a cable system head end consistent with
16 certain embodiments of the present invention.

17 **FIGURE 6** is a flow diagram of a set-top box consistent with certain
18 embodiments of the present invention.

19

20 **ACRONYMS, ABBREVIATIONS AND DEFINITIONS**

21 **ASI** - Asynchronous Serial Interface

22 **CA** - Conditional Access

23 **CASID** - Conditional Access System Identifier

24 **CPE** - Customer Premises Equipment

25 **DHEI** - Digital Headend Extended Interface

26 **ECM** - Entitlement Control Message

27 **EPG** - Electronic Program Guide

28 **GOP** - Group of Pictures (MPEG)

29 **MPEG** - Moving Pictures Experts Group

- 1 **MSO** - Multiple System Operator
- 2 **PAT** - Program Allocation Table
- 3 **PID** - Packet Identifier
- 4 **PMT** - Program Map Table
- 5 **PSI** - Program Specific Information
- 6 **QAM** - Quadrature Amplitude Modulation
- 7 **RAM** - Random Access Memory
- 8 **SAN** - Storage Area Network
- 9 **VOD** - Video on Demand
- 10 **Critical Packet** - A packet or group of packets that, when encrypted, renders a
- 11 portion of a video image difficult or impossible to view if not properly decrypted,
- 12 or which renders a portion of audio difficult or impossible to hear if not properly
- 13 decrypted. The term "critical" should not be interpreted as an absolute term, in
- 14 that it may be possible to hack an elementary stream to overcome encryption of
- 15 a "critical packet", but when subjected to normal decoding, the inability to fully or
- 16 properly decode such a "critical packet" would inhibit normal viewing or listening
- 17 of the program content.
- 18 **Selective Encryption (or Partial Encryption)** – encryption of only a portion of
- 19 an elementary stream in order to render the stream difficult or impossible to use
- 20 (i.e., view or hear).
- 21 **Dual Selective Encryption** – encryption of portions of a single selection of
- 22 content under two separate encryption systems.
- 23 **Passage™** - Trademark of Sony Electronics Inc. for various single and multiple
- 24 selective encryption systems, devices and processes.

25

26 The terms "a" or "an", as used herein, are defined as one, or more than
27 one. The term "plurality", as used herein, is defined as two or more than two.
28 The term "another", as used herein, is defined as at least a second or more. The
29 terms "including" and/or "having", as used herein, are defined as comprising (i.e.,

1 open language). The term "coupled", as used herein, is defined as connected,
2 although not necessarily directly, and not necessarily mechanically. The term
3 "program", as used herein, is defined as a sequence of instructions designed for
4 execution on a computer system. A "program", or "computer program", may
5 include a subroutine, a function, a procedure, an object method, an object
6 implementation, in an executable application, an applet, a servlet, a source code,
7 an object code, a shared library / dynamic load library and/or other sequence of
8 instructions designed for execution on a computer system.

9 The terms "scramble" and "encrypt" and variations thereof may be used
10 synonymously herein. Also, the term "television program" and similar terms can
11 be interpreted in the normal conversational sense, as well as a meaning wherein
12 the term means any segment of A/V content that can be displayed on a television
13 set or similar monitor device. The term "video" is often used herein to embrace
14 not only true visual information, but also in the conversational sense (e.g., "video
15 tape recorder") to embrace not only video signals but associated audio and data.
16 The term "legacy" as used herein refers to existing technology used for existing
17 cable and satellite systems. The exemplary embodiments of fail-safe content
18 encryption and more specifically the decryption elements associated with this
19 technology disclosed herein can be employed in a television Set-Top Box (STB),
20 but it is contemplated that such technology will soon be incorporated within
21 television receivers of all types whether housed in a separate enclosure alone or
22 in conjunction with recording and/or playback equipment or Conditional Access
23 (CA) decryption module or within a television set itself.

24 The term "encryption device" and variations thereof can be interpreted as
25 a component or assemblage of components that implement the system function
26 of providing cryptographic encryption of clear content passing through the device,
27 as well as the creation, processing and insertion of supporting messages, in
28 whole or in part, such as ECMs, etc. The term "decryption device" and variations
29 thereof can be interpreted as a component or assemblage of components that

1 implement the system function of decrypting encrypted content to retrieve the
2 initial clear content.

3

4

DETAILED DESCRIPTION OF THE INVENTION

5 While this invention is susceptible of embodiment in many different forms,
6 there is shown in the drawings and will herein be described in detail specific
7 embodiments, with the understanding that the present disclosure is to be
8 considered as an example of the principles of the invention and not intended to
9 limit the invention to the specific embodiments shown and described. In the
10 description below, like reference numerals are used to describe the same,
11 similar, or corresponding parts in the several views of the drawings.

12 The message traffic between elements of a conditional access system and
13 an encryption device contained within the conditional access management
14 system (typically the cable system head end) is both time critical and non-
15 homogeneously distributed. The encryption device has no idea a priori which
16 services are intended to be encrypted, what the access criteria should be or
17 when it may change. If communication between the encryption device(s) (within
18 the conditional access management system - cable system head end) and the
19 conditional access system is lost, the encryption device will continue to use the
20 last received access criteria information indefinitely and continue to use the
21 current ECM and corresponding encryption key, regardless of cryptoperiod
22 expiration, since no new signed ECMs have been received to replace the one
23 currently being used (stale ECMs). This situation maintains the basic
24 safekeeping of the transmitted content, since encryption continues, but could
25 allow the content to be more easily attacked using empirical methods and
26 possibly recovered since the key is static. It will be understood that the term
27 encryption, as used herein, can be either selective encryption or full encryption
28 without limitation.

1 For pay-per-view services, in the event of a similar communication loss, a
2 paying subscriber will continue to see subsequent programs for free since the
3 access criteria does not change for subsequent programs during a
4 communication loss. With no new access criteria delivered, the subscriber
5 terminals have no indication that a transition from one conditional access event
6 to another has occurred. Restoration of communications will cause the
7 encryption device to renegotiate its connection to the conditional access system
8 and the system will self-restore. Similar results occur if the ECMG or other
9 conditional access management system elements fail after commencement of
10 normal operation.

11 A different scenario occurs if the encryption device is somehow rebooted
12 or reset during a communication loss with the conditional access management
13 system or, if for whatever reason, the encryption device cannot establish
14 communication with the conditional access system during encryption device
15 initialization after any of a reset, or a cold or warm boot. In these cases, there is
16 no previous key and corresponding signed ECM to continue use of. There is no
17 indication available to the encryption device from the conditional access system
18 regarding which services should be encrypted. In current real-world systems, all
19 content is transmitted entirely in the clear in this scenario, and as a result,
20 anyone with the ability to access the cable plant feed will be able to receive those
21 services with full fidelity.

22 In the past, there were virtually no ITU-J.83 compliant receiving/decoding
23 devices available to consumers other than the devices supplied by their cable
24 operator. With the Open Cable initiative and advancements in the computing
25 and consumer electronics industries, many devices are now being offered in the
26 consumer marketplace possessing the ability to both receive and decode
27 unencrypted cable content, further complicating the problem. Any programming
28 transmitted without encryption will thus be easily displayed by those devices,
29 without regard for whether the display is authorized. In the case of adult content

1 or other possibly offensive content, there is no way to limit access only to
2 consenting adults in this scenario if there is no encryption of the content, thereby
3 creating possible legal and public relations issues.

4 One solution to this dilemma is to modify the encryption device to contain
5 in flash memory or any other nonvolatile storage, a list of operator manually
6 configured services indicating which ones may require special consideration due
7 to content (e.g., adult or otherwise objectionable content) or value (e.g., Pay-Per-
8 View, subscription or VOD content) and therefore should always be encrypted. If
9 the encryption device, upon reboot or other initialization, is unable to establish
10 communication with the conditional access management system it automatically
11 begins encryption of the services marked in the configuration table using a
12 predetermined fixed key. No ECM is transmitted while in this state, since none is
13 available (in this particular system state, there is no way to communicate with the
14 conditional access system to have it apply the proprietary algorithm to conceal
15 the content encryption key, therefore and ECM cannot be generated) .

16 By using a default key and suspending any further ECM delivery, no
17 subscriber terminal device will be able to decode the content on the marked
18 streams. While this causes a loss of service in certain situations, it prevents the
19 less desirable situation of uncontrolled delivery of inappropriate content and its
20 ramifications. Once communication is restored or established between the
21 conditional access system and the content encryption device, the encryption
22 device will properly provision and normal key/ECM processing will take place,
23 enabling authorized subscribers to once again be able to access the content.

24 Throughout the following discussion, the above-referenced patent
25 applications can be referenced for specific details of exemplary embodiments of
26 single and multiple partial encryption as it relates to the present disclosure. It is
27 noted that in all cases, full encryption or selective encryption can be enabled
28 using the embodiments described herein.

1 Turning now to **FIGURE 2**, an illustrative Default Multi-channel Encryption
2 System (DMES) 200 is shown. This figure builds on **FIGURE 1**, with the addition
3 of default configuration memory 204 which is used to store default encryption
4 information for situations of communication failure between content encryption
5 block 104 and conditional access system 108. One of the possible multiple
6 conditional access systems within the cable system head end is shown as
7 conditional access system 108. Conditional access system 108 is responsible
8 for, among other things, encrypting the content of each program that is broadcast
9 from the cable system head end. Encryption keys and other related, time-varying
10 information is generated in content encryption block 104 as discussed above and
11 in the published DVB specification. Content encryption block 104 behaves as a
12 conditional access management system.

13 As mentioned above, this encryption information is changed periodically,
14 occasionally, or according to any defined schedule so that content encryption
15 block 104 and conditional access system 108 attempt to remain in
16 communication, subject to the difficulties discussed above, via conditional access
17 system communications link 172.

18 In order to resolve the difficulties associated with a loss or absence of
19 communication between conditional access system 108 and the remainder of the
20 cable system head end, default configuration memory 204 is provided. Default
21 configuration memory 204 can be any non-volatile storage mechanism, such as
22 Flash memory, ROM memory, battery backed up memory, disc storage, or any
23 other suitable computer readable storage medium, so that its contents are
24 persistent through power cycles of the system. Default configuration memory
25 204 is connected to SCS processor 116 via CA memory interface 208.

26 SCS processor 116 can be used during set up and initial provisioning of
27 the cable system head end to provide contents for default configuration memory
28 204, organized on a channel-per-channel basis. A decision can be made by the

1 cable provider regarding the level and type of encryption to be used as a default
2 for all channels provided by the system.

3 Once initialized, the presence of the default configuration memory 204
4 allows content encryption block 104 to read default encryption keys and other
5 related information associated with the cable channels in the event of a
6 communication loss between itself and conditional access system 108.
7 Accordingly, under any of the situations discussed above, content encryption
8 block 104 will always have a capability for encryption using a default encryption
9 key for each cable channel once initialized and provisioned. This prevents
10 broadcast of objectionable and/or premium content (or any other designated
11 content) in the clear to prevent unauthorized recipients from viewing the content.
12 It should be noted that even if the system contains no receiver devices (e.g.,
13 STBs) that are appropriately outfitted (as will be described later) to receive
14 content that is encrypted under the default encryption keys, it is often preferred
15 for paid viewers to have their programming disrupted than to have objectionable
16 or otherwise normally protected content transmitted without benefit of encryption.

17 Thus, an apparatus for default encryption of content for distribution,
18 consistent with certain embodiments, has a conditional access system. A
19 conditional access management system communicates with and manages the
20 conditional access system. A memory device stores default encryption
21 information for use by the conditional access system to encrypt certain content
22 upon a communication failure between the conditional access system and the
23 conditional access management system.

24 Turning now to **FIGURE 3**, an illustrative default encryption information
25 retrieval method 300 is shown. At 304, the method begins. At 308, the process
26 determines whether the communication channel between the conditional access
27 system 108 and the content encryption block 104 is active and functioning
28 properly or whether there has been a communication failure. Note that, in certain
29 embodiments, the attempted communication occurs every few seconds (or

1 faster), so detection of communication loss or restoration may have a very low
2 latency. If a communication failure has not occurred at 308, a transition is made
3 to 312 to carry out communications to transmit encryption keys and related
4 information from content encryption block 104 of cable system head end to
5 conditional access system 108 for all channels in the system. Otherwise, if a
6 communication failure is determined to have occurred at 308, a transition is
7 made to 316 where encryption keys and related information is read from the
8 default configuration memory 204 until communication is restored. The
9 communication channel is again checked at 308 where the process repeats
10 during the current power cycle of the equipment.

11 Turning now to **FIGURE 4**, an illustrative Default Multi-channel Decryption
12 System (DMDS) 400 is shown. To further extend the capability and to
13 accommodate legally authorized STB's to view content scrambled with a fixed
14 key as described above, an alternative embodiment provides for assignment of a
15 default key or keys to the STB (or other receiver device). In this manner, those
16 legally authorized STBs can be signaled and can temporarily use the default
17 fixed key(s) to descramble content until such time as the live keys can again be
18 injected into the stream. One possibility for the signaling is a specially formatted
19 ECM, originating from the encryption device (since the conditional access system
20 108 to the content encryption block 104 connectivity has been lost) and signaling
21 the STB to resort to a fixed-key mode.

22 In this embodiment, which builds upon **FIGURE 2**, STB 112 includes
23 default configuration memory 404 for storing the default fixed key(s), as
24 discussed above which is interfaced to ECM processor 1120 across CA memory
25 interface 408.

26 The default fixed key(s) can be the same for all channels, or can be
27 unique for each, or for a group of channels deemed to have a similar
28 characteristic. Alternatively, there could be separate keys for different classes of
29 programming (sports, adult entertainment, performances, etc.), or in accordance

1 with content rating (G, PG, PG-13, R, X, etc.). As well, the fixed keys can be
2 transmitted during the signaling discussed above or can be fixed within the units
3 during manufacture or installation. In any case, the default configuration memory
4 404 can be any non-volatile memory, such as Flash memory, disc storage,
5 battery backed-up memory, or any other suitable computer readable storage
6 device. Due to the non-volatile nature of the default configuration memory 404,
7 the default fixed key(s) are able to survive a power cycle at the STB 112.
8 Further, by using a one-time programmable memory buried within the decoding
9 device, encryption of the default fixed key(s), or other methods, tampering with,
10 or observation of, the default fixed key(s) can be prevented. As well, secure
11 replacement mechanisms, such as encrypted delivery of new default fixed key(s),
12 are envisioned that prevent tampering or observation of the default fixed key(s)
13 during replacement.

14 Turning now to **FIGURE 5**, an illustrative default encryption information
15 retrieval method 500 is shown. This diagram is very similar to **FIGURE 3** above
16 with the addition of signaling blocks and is carried out at the cable system head
17 end at content encryption block 104. At 504, the method begins. At 508, the
18 process determines whether the communication channel between the conditional
19 access system 108 and the content encryption block 104 is active and
20 functioning properly or whether there has been a communication failure. If a
21 communication failure has not occurred at 508, a transition is made to 512 to
22 carry out communications to transmit encryption keys and related information
23 from content encryption block 104 to conditional access system 108 for all
24 channels in the system. Then at 516, a global signaling to the STBs in the
25 system is done to instruct the STBs to extract encryption keys from the data
26 stream.

27 If a communication failure is determined to have occurred at 508, a
28 transition is made to 520 where encryption keys and related information are read
29 from the default configuration memory 204 at the content encryption block 104 of

1 the cable system head end until communication is restored. At 524, a global
2 signaling to the STBs in the system is done to instruct the STBs to switch to the
3 default fixed key(s) as discussed above. The communication channel is again
4 checked at 508 where the process repeats during the current power cycle of the
5 equipment.

6 Turning now to **FIGURE 6**, an illustrative default multi-channel decryption
7 method 600 is shown. With the signaling discussed above in relation to **FIGURE**
8 **5** implemented at cable system head end, this process can be used within the
9 STB to switch between the signaled active decryption key(s) and default fixed
10 key(s). The process begins at 604. At 608, signaling is received from the
11 content encryption block 104 of the cable system head end. As discussed
12 above, this signaling could include the active key(s), new fixed default key(s) to
13 overwrite those stored in memory, and instructions regarding which set of keys to
14 use.

15 In the case of a communication failure between the content encryption
16 block 104 and the conditional access system 108, no valid active key(s) would be
17 received. In this case, fixed default key(s) and/or instructions to switch to using
18 the default fixed key(s) are provided. Likewise, new fixed default key(s) can be
19 transmitted based upon the decisions of the cable system provider even without
20 a communication failure in the content encryption block 104. At 612, a
21 determination is made as to whether there are new fixed default key(s). If there
22 are, they can be stored to memory at 616. If there are no new default fixed
23 key(s) to store at 612 or the storage is complete at 616 a transition is made to
24 620.

25 At 620, a test is done to determine whether the signaling received at 608
26 contains instructions to switch to using fixed default key(s). If there were no
27 instructions to switch to using fixed default key(s), processing continues normally
28 with received active key(s) at 624. If, however, there were instructions received
29 at 608 instructing the STB to switch to the use of fixed default key(s), a transition

1 is made to 628 to read fixed default key(s) from memory and processing
2 continues normally with the use of the fixed default key(s). The process repeats
3 during the current power cycle of the equipment.

4 Thus, in the event of a power failure or other reboot of the system,
5 programming content can be resumed in a manner that will assure encryption of
6 any desired content, such as for example, all content on certain channels (e.g.,
7 pay channels or channels that may carry content having a rating greater than or
8 equal to an R rating). This prevents unauthorized viewing of these channels.

9 Those skilled in the art will recognize that the present invention has been
10 described in terms of exemplary embodiments based upon use of a programmed
11 SCS processor such as SCS processor 116. However, the invention should not
12 be so limited, since certain embodiments could be implemented using hardware
13 component equivalents such as special purpose hardware and/or dedicated
14 processors which are equivalents to the invention as described and claimed.
15 Similarly, general purpose computers, microprocessor based computers, micro-
16 controllers, optical computers, analog computers, dedicated processors and/or
17 dedicated hard wired logic may be used to construct alternative equivalent
18 embodiments.

19 Those skilled in the art will also appreciate that the program processes
20 and associated data used to implement the embodiments described above can
21 be implemented using disc storage as well as other forms of storage such as for
22 example Read Only Memory (ROM) devices, Random Access Memory (RAM)
23 devices; optical storage elements, magnetic storage elements, magneto-optical
24 storage elements, flash memory, core memory and/or other equivalent storage
25 technologies without departing from the present invention. Such alternative
26 storage devices should be considered equivalents.

27 Certain embodiments can be implemented using a programmed processor
28 executing programming instructions that are broadly described above in flow
29 chart form that can be stored on any suitable electronic storage medium or

1 transmitted over any suitable electronic communication medium. However, those
2 skilled in the art will appreciate that the processes described above can be
3 implemented in any number of variations and in many suitable programming
4 languages without departing from the present invention. For example, the order
5 of certain operations carried out can often be varied, additional operations can be
6 added or operations can be deleted without departing from certain embodiments
7 of the invention. Error trapping can be added and/or enhanced and variations
8 can be made in user interface and information presentation without departing
9 from the present invention. Such variations are contemplated and considered
10 equivalent.

11 While the invention has been described in conjunction with specific
12 embodiments, it is evident that many alternatives, modifications, permutations
13 and variations will become apparent to those skilled in the art in light of the
14 foregoing description. Accordingly, it is intended that the present invention
15 embrace all such alternatives, modifications, permutations and variations as fall
16 within the scope of the appended claims.

17 What is claimed is:
18